UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DAVID DE MEDICIS, on behalf of himself and all others similarly situated,

Plaintiff,

v.

ALLY BANK and ALLY FINANCIAL INC.,

Defendants.

Case No. 21-cv-6799-NSR

ORAL ARGUMENT REQUESTED

MEMORANDUM OF LAW IN SUPPORT OF <u>DEFENDANTS' MOTION TO DISMISS THE AMENDED COMPLAINT</u>

SIMPSON THACHER & BARTLETT LLP
425 Lexington Avenue
New York, New York 10017
Telephone: (212) 455-2000
Facsimile: (212) 455-2502

Attorneys for Defendants Ally Bank and Ally Financial Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

Defendants Ally Bank and Ally Financial Inc. (together, "Ally" or "Defendants"), by and through their undersigned counsel, respectfully submit this memorandum of law in support of their motion to dismiss the Amended Class Action Complaint (the "Amended Complaint"[1]) of Plaintiff David De Medicis ("Plaintiff"), pursuant to FRCP 12(b)(1) and 12(b)(6).

PRELIMINARY STATEMENT

After giving him every benefit of the doubt and drawing every inference in his favor, the Court dismissed Plaintiff's original complaint (the "Original Complaint") in its entirety because he failed to allege any cognizable injury and thus lacked Article III standing. *See De Medicis v. Ally Bank*, 2022 WL 3043669 (S.D.N.Y. Aug. 2, 2022) (the "MTD Decision"). Months later, Plaintiff filed the Amended Complaint, attempting to salvage his case.[2] But nothing in the Amended Complaint requires reconsideration of the MTD Decision, and the Amended Complaint should be dismissed—with prejudice—for the same reasons the Court faulted the Original Complaint. Plaintiff *still* fails to establish either a concrete injury or substantial risk of future injury and *still* fails to link any of the purported harms to the Coding Error (defined below).

As the Court knows, this case involves an inadvertent, computer-programming-code error that occurred when some customers logged into Ally's website (the "Coding Error"). The Coding Error, which happened only under certain circumstances and not in every instance of a customer login, caused certain usernames and passwords embedded in a lengthy string of code to be transmitted to certain businesses that perform services for Ally. Immediately after discovering the Coding Error, Ally fixed the code and forced all potentially impacted passwords to be reset.

[1] Citations to "AC" refer to the Amended Complaint (Dkt. 45), filed January 9, 2023.

[2] Plaintiff filed an initial attempt at an amended complaint on October 18, 2022 (Dkt. 31) without seeking the Court's leave. After Defendants submitted a letter-motion in anticipation of asking the Court to strike it or in the alternative dismiss it for the same reasons as the Original Complaint, Plaintiff voluntarily withdrew that complaint and sought leave to file, which the Court granted on December 20, 2022 (Dkt. 44). Plaintiff then filed the Amended Complaint at issue on this motion, asserting additional allegations not included in the October version.

Additionally, each of the businesses that work with Ally deleted the information. Ally also immediately began and continues targeted fraud-monitoring efforts of the impacted customer population. Ally's prompt response was successful—not a single instance of identity theft or fraud attributable to the Coding Error has been identified. Put simply, the inadvertent error has not caused *any* harm to *any* of Ally's customers, including Plaintiff.

The Court previously rebuffed Plaintiff's attempt to hold Ally liable simply because the Coding Error occurred, and it should do so again for three overarching reasons. *First*, the Amended Complaint should be dismissed under Rule 12(b)(1) because Plaintiff lacks Article III standing and thus this Court lacks subject matter jurisdiction. Article III standing requires either a present injury or a substantial likelihood of future injury. Plaintiff has pled neither. As to present injury, the Amended Complaint largely reiterates those the Court previously rejected, including the "time spent" monitoring his accounts and exploring credit monitoring and identity theft protection, and "attempts" by "hackers" to access his email and sports-betting accounts. Plaintiff's other allegations relating to certain Ally "account freezes" and reimbursed charges on non-Ally accounts are not cognizable injuries and, therefore, fail as a matter of law. As to future injury, as he did the first time around, Plaintiff fails on all three of the *McMorris* factors the Second Circuit identified (and this Court previously applied) as determinative in cases premised on a theory of future harm: specifically, (i) the exposure was due to an inadvertent error rather than to malicious hackers, (ii) the exposed information has not been misused, and (iii) the exposed information was not sensitive or high risk (and was immediately changed through a forced password reset). Indeed, Plaintiff's claimed risk hypothetical future injuries—which the Court previously rejected—is even weaker now, including because of the passage of even *more* time in which no harm has befell Plaintiff or *any other Ally customer* as a result of the Coding Error. No injury, no standing.

Second, irrespective of injury, Plaintiff also lacks Article III standing because he fails to demonstrate any nexus between the Coding Error and his alleged injuries. Nor could he, as Defendants have again submitted dispositive evidence demonstrating otherwise. Moreover, not only are the purported injuries so distant in time (as this Court previously recognized), but there is a casual break in his allegations. In his Amended Complaint, Plaintiff admits to reusing passwords—including his Ally password—across multiple other sites, including Amazon and Coinbase. Further, Plaintiff's sensitive personal information has been implicated in at least *25 distinct and independent data breaches*—some perpetrated by malicious hackers and none of which involve Ally—compromising everything from his email, passwords, password hints, usernames, phone numbers, physical addresses, date of birth, IP addresses, and partial credit card data. It is utterly implausible that his alleged injuries stem from the Coding Error (which was limited only to Ally business partners and rectified immediately) and not one of these malicious breaches.

Finally, even if Plaintiff had Article III standing (he does not), each of his seven claims should be dismissed under Rule 12(b)(6). Not only does he fail to allege damages (*i.e.*, injury)—which is a higher standard than constitutional injury—but he also fails to allege the required elements for *any* of his claims. Plaintiff's negligence, negligence *per se* claim, implied contract duty, North Carolina Unfair & Deceptive Trade Practices Act, Virginia Personal Information Breach Notification Act, and declaratory/injunctive relief claims accordingly all fail.

Under either Rule 12(b)(1) or 12(b)(6), the Amended Complaint must be dismissed.

FACTUAL BACKGROUND

A. The parties.

Ally Financial Inc. is a leading digital financial-services company that provides a variety of financial services to more than 8.5 million consumer, commercial, and corporate customers. Its wholly owned subsidiary, Ally Bank, is an award-winning digital direct bank that offers mortgage lending, point-of-sale personal lending, and a variety of other banking and investment products.[3]

Plaintiff "is a Virginia resident." AC ¶ 19. He maintains "checking, savings and securities accounts" with Ally. *Id.*

B. The Coding Error.

On April 12, 2021, during a routine website update, Ally learned of an inadvertent coding error affecting certain query strings that transmit information after a customer entered a username and password to access an Ally account. *Id.* at ¶ 1; Decl. ¶ 4.[4] These query strings usually do not contain any personally identifiable information. *Id.* ¶ 6. The Coding Error, however, resulted in certain query strings that potentially contained usernames and passwords (embedded within the string) being sent to a limited group of known entities with which Ally has ongoing contractual and business relationships. *Id.* ¶ 7. The following is an actual (redacted) query string:

```
https://www.ally.com,/,/,/?hdmjavascriptdata=&allysf-login-v1-account=aaos&allysf-login-
v1-username-78e30d704ccce8ccc7b8539f0144cb09=[redacted]&allysf-login-v1-password-
78e30d704ccce8ccc7b8539f0144cb09=[redacted]
```

Id. ¶ 10. The Coding Error only occurred in limited circumstances where the user attempted to log in before the page had fully loaded (*e.g.*, if the user was using software to automatically populate the username and password). *Id.* ¶ 7.

In order to actually access an Ally online account, a person at one of the entities to which the strings were visible would have had to first ascertain that a query string could have included a username and password, and would then have had to parse the information from within the string. *Id.* ¶ 9. Not all usernames and passwords in the query strings, moreover, would have necessarily

[3] *See* 2020 10-K Annual Report, Ally Financial Inc. (Feb. 24, 2021) at 5.

[4] References to "Decl. ¶ __" refer to the Declaration of Christian Hall, submitted herewith.

contained correct or complete usernames or passwords; for example, if a customer had incorrectly typed the username or password, that incorrect information would have been embedded in the string, and the information could not be used to gain access to an account. *Id.*

C. Ally eliminates the Coding Error and assesses the potential impact.

Immediately upon learning of the Coding Error, Ally updated the affected code to eliminate the error. AC ¶ 10; Decl. ¶ 13. Ally also implemented a process that required all potentially affected customers—whether or not they were actually affected—to change their password. *Id.* ¶ 14. Plaintiff changed his password on April 15, 2021. *Id.* ¶ 24.

Additionally, Ally immediately began working with the businesses to which the query strings may have been visible to purge the information. *Id.* ¶ 15. All of these entities agreed to delete the information, and all subsequently confirmed deletion. *Id.*

Ally also immediately began the process of determining which customers' usernames and passwords may have been embedded in the query strings as a result of the Coding Error. *Id.* ¶ 17. To do this, Ally had to parse millions of website login attempts and, for each login attempt, identify whether the Coding Error had actually occurred during the login attempt (because, as noted above, it only occurred in certain circumstances) and, if so, match the information to a specific customer. *Id.* Ultimately, Ally identified each potentially impacted customer. *Id.* ¶ 18.

Ally also immediately began fraud-monitoring efforts to assess threats or risks of fraud specific to the Coding Error, including monitoring the accounts of potentially affected customers for fraudulent, suspicious, or anomalous activity. *Id.* ¶ 16.

D. Ally promptly notifies potentially impacted customers of the Coding Error.

After identifying which customers' information had been embedded in the query strings as a result of the Coding Error, Ally sent each customer a letter explaining the circumstances of the error. *Id.* ¶ 19. This letter, dated June 11, 2021, explained the remedial steps that Ally had taken as quickly as possible after discovering the Coding Error, including (1) updating the code; (2) requiring customers to reset their passwords; (3) confirming that all third parties would delete the information; and (4) monitoring customers' accounts. *See* Decl. Ex. B. Additionally, although the risk of potential fraud was low given the circumstances of the Coding Error and the steps that Ally immediately took, Ally offered all affected customers free credit monitoring and identity theft insurance coverage for two years. *See id.*; AC ¶ 123.

E. Ally identifies no fraudulent activity as a result of the Coding Error.

Since discovery of the Coding Error on April 12, 2021, Ally's internal cyber risk and fraud teams have monitored the accounts of the customers affected by the Coding Error for any increase in potential fraudulent or other anomalous activity. Decl. ¶ 22. Ally has identified no instances of account takeovers, identity theft, or other fraud attributable to the Coding Error. *Id.* ¶ 23. Additionally, Ally has not identified any increased rates of potentially fraudulent activity or other anomalous events attributable to the Coding Error; in other words, the rate of potentially fraudulent activity across the population of affected accounts has remained in line with that of unaffected customer accounts. *Id.*

F. The Original Complaint.

On August 12, 2021, Plaintiff filed the Original Complaint, alleging five causes of action: negligence, negligence *per se*, breach of implied contract, violation of the Virginia Personal Information Breach Notification Act, and injunctive/declaratory relief under the Declaratory Judgment Act. *See* Orig. Compl. ¶¶ 60–99. Plaintiff claimed he was "harmed" by the Coding Error because he "devot[ed] time" to "self-monitoring his accounts" and "changing the password and usernames on many of his personal online accounts," and suffered "diminution in the value of his private information" as well as "lost time, annoyance . . . and inconvenience." *Id.* ¶¶ 31–34. Plaintiff also alleged he had experienced three "attempts by hackers to reset the password of his email account without his knowledge or permission." *Id.* ¶ 51.

G. Defendants' motion to dismiss the Original Complaint.

Defendants moved to dismiss the Original Complaint under Rules 12(b)(1) and 12(b)(6). *See* MTD (Dkt. 19). As to Rule 12(b)(1), Defendants argued that Plaintiff lacked Article III standing because he failed to allege (a) a present injury or (b) a substantial risk of future injury. In opposition, Plaintiff asserted new purported harms. *See* Pl.'s Decl. (Dkt. 22). He claimed anew that after April 2021, multiple attempts were made to access his FanDuel account and his email, which utilized a "similar" username as his Ally account; that one attempt was made to access his Ally account in September 2021; and that, prior to that, Ally locked him out of his account for roughly ten days in August 2021. *Id.* ¶¶ 4–9. In reply, Ally showed that none of these new supposed "injuries" were related to the Coding Error. *See* MTD Reply (Dkt. 23) at 2–3.

H. The MTD Decision dismissing the Original Complaint.

The Court dismissed Plaintiff's Original Complaint in a detailed, nineteen-page decision. The Court rejected Plaintiff's three purported present injuries as insufficient for Article III standing: namely, (1) the "time spent" monitoring his accounts, "exploring credit monitoring and identity theft protection," and changing his passwords and usernames on various online accounts, (2) the "diminution in the value" of his private information, and (3) the "three attempts by hacker[s] to reset the password of his email account without his knowledge or permission." *See* MTD Decision at *5–6. The Court also found, applying the Second Circuit's three-factor *McMorris* test (discussed below), that Plaintiff failed to allege a substantial risk of future injury because (i) "the Coding Error was inadvertent and the result of a programming error . . . rather than a sophisticated attack perpetrated by cyber criminals or state sponsored hackers," (ii) Plaintiff failed to allege that "the Coding Error resulted in any actual misuses of his username and password," and (iii) "the private information allegedly disseminated" (specifically, "Plaintiff's username and password") was not "high-risk information" and could be "rendered useless to cybercriminals [and] does not pose the same risk of future identity theft or fraud to plaintiffs if exposed." *Id.* at *9–10.

The Court further noted that Plaintiff had inappropriately submitted new allegations in an effort to "shore up" the deficiencies in the Original Complaint. *Id.* at *8. Nevertheless, the Court evaluated these new allegations and concluded that all "such allegations . . . fail[ed]." *Id.* First, Plaintiff failed to establish a plausible casual connection between the email and FanDuel "hacks" and the Coding Error. *Id.* "[E]ven when taken as true," the Court explained, these allegations "at best" established only an "implied temporal connection"—the "attempts" happened roughly six months after the Coding Error—but were inadequate to establish the necessary *non-temporal* nexus between the two incidents. *Id.* at *7–8 (citing *Stollenwerk v. Tri–West Health Care Alliance*, 254 F. App'x 664 (9th Cir. 2007)). Second, the Court credited Defendants' unrebutted evidence that (1) the notification Plaintiff received of an attempted access to his Ally account actually resulted from failed log-in attempts by financial aggregators that Plaintiff himself used to link other online accounts to his Ally accounts; and (2) Plaintiff temporarily lost access to his Ally account after he commenced his suit because Ally instituted a legal preservation hold that is intended to prevent any record purges for purposes of litigation—and not because of "hackers" attempting to login into his account. *Id.* at *8. Accordingly, the Court held that Plaintiff failed to establish the injury requirements for Article III standing and dismissed the Original Complaint pursuant to Rule 12(b)(1). *See id.* at *10. It did not reach Ally's arguments under Rule 12(b)(6). *See id.*

I. **The Amended Complaint**.

The Amended Complaint includes the original five causes of action and two new causes of action: breach of fiduciary duty and violations of the North Carolina Unfair & Deceptive Trade Practices Act. It asserts the same supposed "harms" already rejected by the Court. It also adds three new supposed injuries: namely, allegations of unauthorized (non-Ally) account access, restrictions on Ally account access, and unauthorized (non-Ally) transactions. *See* AC ¶¶ 109–115. These new alleged "injuries" include unauthorized access to and transactions using his Coinbase and Amazon accounts, both of which purportedly used the same Ally password utilized by Plaintiff at the time of the Coding Error, and restrictions on his Ally accounts because of suspicious activity. *See id.* ¶ 109, 113–14. The Amended Complaint also points to anonymous and unverified Ally customer complaints over the eighteen months following the Coding Error, which Plaintiff claims "demonstrates" that the Coding Error caused a "wave" of unauthorized transactions. *See id.* ¶¶ 14, 98–106.

ARGUMENT

I. THE AMENDED COMPLAINT MUST BE DISMISSED UNDER RULE 12(b)(1) BECAUSE PLAINTIFF LACKS ARTICLE III STANDING.

A. Legal standard.

Dismissal is proper under Rule 12(b)(1) for lack of subject matter jurisdiction where the plaintiff lacks Article III standing because "[i]f plaintiffs lack Article III standing, a court has no subject matter jurisdiction to hear their claim." *Cent. States So. & Sw. Areas Health & Welfare Fund v. Merck-Medco Managed Care, L.L.C.*, 433 F.3d 181, 198 (2d Cir. 2005). "A plaintiff asserting subject matter jurisdiction has the burden of proving by a preponderance of the evidence that jurisdiction exists." *Clarex Ltd. v. Natixis Secs. Am. LLC*, 2012 WL 4849146, at *2 (S.D.N.Y. Oct. 12, 2012) (noting that "jurisdiction must be shown affirmatively" (quoting *Giammatteo v. Newton*, 452 F. App'x 24 (2d Cir. 2011))).

On a 12(b)(1) motion to dismiss, a defendant may proffer evidence beyond the complaint in the form of factual declarations. *See Katz v. Donna Karan Co., L.L.C.*, 872 F.3d 114, 119 (2d Cir. 2017). The plaintiff will need to "come forward with evidence of [his] own to controvert" defendants' evidence. *Id.* If the defendant's evidence is "material and controverted," the court must make factual findings to determine whether the plaintiff has standing. *Id.* at 120.

To establish "the irreducible constitutional minimum" of Article III standing, a plaintiff must demonstrate (1) "an injury in fact to a legally protected interest that is both (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical"; (2) that the defendant caused the injury; and (3) that it is "likely" that the requested relief would "redress" the injury. *See Crupar-Weinmann v. Paris Baguette Am., Inc.*, 861 F.3d 76, 79 (2d Cir. 2017) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992)). Plaintiff fails on injury and causation.[5]

B. Plaintiff does not allege and cannot demonstrate a *present* injury.

To satisfy the "injury in fact" element for cases involving allegations of "unauthorized exposure of th[e] plaintiff's data, the complaint must establish either a present injury or a future injury due to the alleged exposure." MTD Decision at *4 (citing *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 300–01 (2d Cir. 2021)). The Amended Complaint alleges five categories, or buckets, of supposed present injuries. The Court has already considered and rejected the bulk of these, and the remainder similarly fail under the Court's prior analysis.

The first bucket relates to unsuccessful attempts by alleged "hackers" to access some of Plaintiff's online accounts, namely, (1) his Ally Bank accounts on September 11, 2021, (2) his email account "[s]hortly after September 11, 2021," and (3) his FanDuel account on November 16, 2021. AC ¶¶ 85, 87, 89. As the Court has already determined, such "attempts" are not a cognizable injury. *See* MTD Decision at *6 (holding that Plaintiff failed to establish a concrete injury because alleged attempts "were all unsuccessful"); *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90 (2d Cir. 2017) (attempted fraud insufficient to constitute injury).

[5] Because Plaintiff fails to satisfy the first or second prong, the Court need not address the third. *See, e.g.*, *Garelick v. Sullivan*, 987 F.2d 913, 919 (2d Cir. 1993).

The second bucket relates to the time and effort Plaintiff allegedly spent "ascertain[ing], migrat[ing] and remediat[ing]" the "adverse impacts on his privacy, his identity, and security of his financial and other accounts." AC ¶¶ 93–96, 113. These, however, do not constitute a present injury sufficient to supply standing absent a substantial risk of future identity theft. *See McMorris*, 995 F.3d at 303. As explained *infra* Section I.C, for the same reasons the Court previously recognized, there is no such risk here. MTD Decision at *10 ("Plaintiff fails to plausibly allege a substantial risk of future injury resulting from the Coding Error.").

The third bucket relates to unauthorized transactions allegedly made on Plaintiff's Coinbase and Amazon accounts. As to Coinbase, Plaintiff alleges that on October 21, 2022, a "malicious actor broke into [his] Coinbase account" and "spent down the total value of cryptocurrency then on deposit in [that] account" before "attempting" to initiate an additional transfer from his Wells Fargo account to his Coinbase account. AC ¶ 109. As to Amazon, Plaintiff alleges that on or before October 28, 2022, a "fraudster hacked [his] Amazon account" and "attempted purchases" with the credit cards on file with that account. *Id.* ¶ 114. In both cases, Plaintiff concedes that the unauthorized transactions were refunded. *Id.* ¶¶ 112, 115. Though the Court did not have opportunity to address these particular allegations in the MTD Decision, the Court rightly noted that "attempted fraud [is] insufficient to constitute injury." MTD Decision at *6 (describing *Whalen*, 689 F. App'x at 90). Refunded or reversed transactions like these do not constitute an injury in fact for standing purposes. *See, e.g.*, *Whalen v. Michael Stores Inc.*, 153 F. Supp. 3d 577, 580 (E.D.N.Y. 2015), *aff'd*, 689 F. App'x 89 (2d Cir. 2017) (no standing because plaintiff had not alleged "that she suffered any unreimbursed charges"); *Torres v. Wendy's Co.*, 195 F. Supp. 3d 1278, 1283 (M.D. Fla. 2016) ("Plaintiff has not alleged that the two fraudulent charges went unreimbursed by his credit union and has experienced no additional actual harm since then.”). In any event, even taking Plaintiff's allegations of alleged harm in his Coinbase and Amazon accounts on their face, there is no causal link to the Coding Error. *See infra* Section I.D.

The fourth bucket relates to alleged restrictions on account access. Specifically, Plaintiff alleges that his Ally accounts were “froze[n]” in August 2021 and twice since October 2022. AC ¶¶ 76, 113. The Court has already recognized that the August 2021 “freeze” was not due to the Coding Error (*see* MTD Decision at *8), and the post-October 2022 “lock-outs,” which the Court has not yet had an opportunity to address, likewise are not an injury. It is well settled that the bare inability to access an account temporarily is not an injury in fact. *See, e.g.*, *Rudolph v. Hudson's Bay Co.*, 2019 WL 2023713, at *8 (S.D.N.Y. May 7, 2019) (“Absent an allegation of how an account freeze resulted in a loss to [plaintiff], the claim that she was injured by the temporary inability to access her account does not demonstrate injury.”).

The fifth and final bucket relates to Plaintiff's alleged loss of the abstract “opportunity” to invest at advantageous prices sometime between August 18 and 27, 2021. *See* AC ¶¶ 76, 82. Specifically, Plaintiff alleges that “Ally's freezing of [his] accounts robbed” [him] of the opportunity to purchase securities at advantageous market prices, such as the Vanguard Russell 1000 Growth ETF,” because it “prohibited [him] from transferring funds on deposit in his Ally Bank checking/savings account to his Ally Invest securities trading account.” *Id.* ¶¶ 80, 82. Critically, as noted above, the Court has already recognized that the August 2021 “freeze” is not due to the Coding Error. Moreover, Plaintiff does not allege that he was *going to* invest but-for the account freeze; rather, he alleges only that he was “robbed” of “the *opportunity*” to invest. *See id.* ¶ 82 (emphasis added). The mere fact that one could have invested is not a concrete injury in fact for standing purposes absent an actual intent to do so. *See Rosario v. Icon Burger Acquisition LLC*, 2022 WL 198503, at *3 (E.D.N.Y. Jan. 21, 2022) (“[A]bsent factual allegations that the plaintiff forewent the opportunity to invest . . . he cannot plausibly claim he suffered a harm sufficiently concrete to establish Article III standing."). Plaintiff pleads no such actual intent.

In short, Plaintiff fails to establish a present injury in fact stemming from the Coding Error.

C. Plaintiff does not allege and cannot demonstrate a substantial risk of *future* injury.

A risk of future injury may also satisfy the "injury in fact" requirement, but only "if the threatened injury is *certainly impending*, or there is a *substantial risk* that the harm will occur." *McMorris*, 995 F.3d at 300–01 (emphasis added). In *McMorris*, the Second Circuit held that Article III standing in an "unauthorized data disclosure" action could be based on a "substantial risk of future identity theft or fraud." *Id.* at 300, 303. It identified three factors that "bear on whether the risk of identity theft or fraud is sufficiently 'concrete, particularized, and . . . imminent'" for purposes of Article III standing in data-exposure cases. *See id.* at 301. As the Court previously recognized (MTD Decision at *9–10) all three *McMorris* factors, when considered against the facts here, weigh against a finding of "substantial risk of future identity theft or fraud." Nothing in the Amended Complaint alters this well-considered conclusion.

1. The Coding Error was inadvertent, not the result of a targeted attack.

The first—and "most important[]"—*McMorris* factor deals with whether "the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data." *McMorris*, 995 F.3d at 301, 303. As Plaintiff concedes and the Court has already recognized, the Coding Error was due to an inadvertent programming error in Ally's website, not any sophisticated attack perpetrated by cyber criminals or state-sponsored hackers. *See* MTD Decision at *9 (Plaintiff "fail[s] to present evidence or make any allegations that an unauthorized third party purposefully obtained [his] data . . . [so] the first *McMorris* factor "weighs against [him]."); AC ¶¶ 45, 48 (describing the issue as a "malfunctioning website"); *see also* Decl. ¶ 4.

2. The transmitted information has not been misused.

The second *McMorris* factor deals with whether "any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud." *McMorris*, 995 F.3d at 303. As an initial matter, the alleged "misuse" of Plaintiff's data is plainly not traceable to the Coding Error, as detailed *infra* Section I.D. Moreover, the anonymous online posts purported to be written by other Ally customers describing unauthorized or declined transactions between April 2021 and October 2022, including a "wave" of such transactions in August 2022, likewise have no plausible link to the Coding Error. AC ¶¶ 14, 16, 98–107.

First, immediately upon discovery the Coding Error, Ally implemented a process that required all potentially affected customers—whether or not they were actually affected—to change their password. Decl. ¶ 14. This means any exposed credentials were "rendered useless to cybercriminals" (MTD Decision at *10) so there can be no misuse stemming from the Coding Error after Ally initiated the mandatory password reset on April 12, 2021.

Second, all but one of the customer complaints do not relate to the type of data at issue here—namely, Ally account usernames and passwords.[6] *Compare, e.g.*, AC ¶ 45 (alleging the dissemination of account credentials), *with* Ex. 1 (excerpted at AC ¶ 14) (reporting unauthorized use of debit card).[7] Instead, as Plaintiff himself acknowledges, they relate to the unauthorized use of credit and debit card information. *See, e.g.*, AC ¶¶ 14, 98 (alleging a "wave of . . . unauthorized transactions on Ally Bank debit and credit cards"). This difference severely undermines any suggestion that the Coding Error caused the unauthorized transactions in the anonymous posts.[8]

[6] The sole instance of alleged credential misuse cited in the Amended Complaint is from October 19, 2021. *See* AC ¶ 14; Ex. 2. But Plaintiff still fails to connect that instance to the Coding Error because Ally had forced a reset of all potentially affected customers' passwords six months earlier. If a third party had this customer's then-current password, it could not have been because of the Coding Error.

[7] References to "Ex. __" refer to exhibits to the Affirmation of Rachel S. Sparks Bradley, submitted herewith.

[8] "To be sure, Plaintiff does allege that access to an online account with Defendants through the disclosed

Stollenwerk v. Tri-West Health Care Alliance, 254 F. App'x 664, 667 (9th Cir. 2007) ("[T]he fact that the *type of information* contained on the stolen hard drives is the same kind needed to open credit accounts at the firms where these incidents took place" could give rise to "inferences . . . establishing causation." (emphasis in original)); *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1326–27 (11th Cir. 2012) (same).

Third, it is facially apparent that these customers were not affected by the Coding Error. For example, with respect to the supposed "wave" of unauthorized card transactions in August 2022, Plaintiff cites an article from Ars Technica (AC ¶ 100 n.22), which discussed two Ally customers who had their debit cards used by a fraudster for test transactions with a small business (*see* Ex. 3 at 6). These customers did not open their accounts with Ally until March 2022—*i.e.*, almost a year *after* Ally corrected the Coding Error. *See id.* It is therefore impossible for the fraudulent activity in August 2022 to have stemmed from Coding Error rectified in April 2021. In a similar vein, consider that not one of the customer posts cited in the Amended Complaint refers to Ally's June 11, 2021 letter disclosing the Coding Error. *See* AC ¶¶ 14, 106. If these customers were affected by the Coding Error, they would have received that letter. But these customers claim the opposite: that "*Ally has not told me (or anyone) about the issue*." *Id.* ¶ 106 (emphasis added).

Fourth, the substantial lapse of time between the Coding Error and the customer posts cited in the Amended Complaint strongly suggests that the former did not cause the latter. *See* MTD Decision at *7–8 (finding that the longer the time span between an alleged data breach and identity theft, the weaker the casual inference and "given that the time gap between the Coding Error and the unsuccessful login attempt here was about six months . . . Plaintiff's allegations . . . are the

usernames and passwords could lead to access to highly sensitive personal identifying information," ostensibly including credit and debit card numbers, but "nowhere does Plaintiff allege that any such access ever in fact occurred with respect to his account or those of Defendants' other customers." MTD Decision at *6.

more inadequate to establish a sufficient non-temporal nexus" (citing *Resnick*, 693 F.3d at 1327)). Ally corrected the Coding Error in April 2021. AC ¶ 10. The "wave" of unauthorized credit and debit card transactions did not occur until August 2022—*sixteen months later*. *Id.* ¶ 98.

Fifth, there are a slew of alternative explanations for the customer issues cited in the Amended Complaint that are wholly unrelated to the Coding Error. The unauthorized credit and debit card transactions in August 2022, for instance, were widely reported to be part of a BIN attack.[9] And many online news outlets have noted that spam, phishing attacks, and other malicious online activity are on the rise.[10] These types of attacks are common, constant, and affect virtually every large business with a virtual presence.[11]

Finally—and crucially—Ally has vigilantly monitored the accounts of its customers affected by the Coding Error. *See* Decl. ¶ 22. To date, it has identified *no* instances of account takeovers, identity theft, or similar occurrences attributable to the Coding Error. *See id.* Additionally, Ally has not identified any increased rates of potentially fraudulent activity or other anomalous events attributable to the Coding Error. *See id.* ¶ 23.

For these reasons, the second *McMorris* prong cuts decisively against a finding that "threatened injury is certainly impending." *McMorris*, 995 F.3d at 300.

[9] In a BIN attack, hackers first obtain the first four to six numbers of a customer's debit card. These numbers are referred to as bank identification numbers, which are the same for all of a bank's debit cards. Thus, a hacker needs only to have or view any Ally Bank debit card to determine the bank's bank identification number. *See Claims of Ally Bank Debit Card Fraud Skyrocket Following Apparent Cyberattack*, JD Supra (Aug. 31, 2022), https://www.jdsupra.com/legalnews/claims-of-ally-bank-debit-card-fraud-7934635/; *Visa Guidance to Guard Against Enumeration Attacks and Account*, Visa Business News (Aug. 12, 2021), https://usa.visa.com/content/dam/VCOM/global/support-legal/documents/visa-guidance-to-guard-against-enumeration-attacks.pdf.

[10] *See, e.g.*, *Over 255m phishing attacks in 2022 so far*, Security Magazine (Oct. 26, 2022), https://www.securitymagazine.com/articles/98536-over-255m-phishing-attacks-in-2022-so-far.

[11] *See* Fed. Trade Comm'n, *New FTC Data Show Consumers Reported Losing Nearly $8.8 Billion to Scams in 2022* (Feb. 23, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022; Fed. Trade Comm'n, *Consumer Sentinel Network Data Book 2022* (Feb. 2023) at 4, https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf.

3. The transmitted information was neither "sensitive" nor "high risk."

The third *McMorris* factor deals with whether "the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud." *Id.* at 303. As this Court has already recognized, and as Plaintiff concedes, it was his sign-in credentials—*i.e.*, his username and password—and not any sensitive and actionable personally identifiable information, such as his name, birthdate, or Social Security Number, that was potentially made visible to certain third parties as a result of the Coding Error. *See* AC ¶ 45; MTD Decision at *10 ("[A]s alleged, Plaintiff's username and password appears to be less sensitive information that can be rendered useless to cybercriminals."). This disposes of the third factor: exposure of usernames and passwords does not present a high risk of identity theft or fraud because both can easily be changed. And indeed, upon discovering the Coding Error, Ally immediately forced all potentially affected customers to reset their passwords, and Plaintiff did so. Decl. ¶ 24. Furthermore, Plaintiff has changed his password over five times since the Coding Error and his username once. *See id.* In contrast to the "dissemination of high-risk information such as Social Security numbers and dates of birth – especially when accompanied by victims' names," which "makes it more likely that those victims will be subject to future identity theft or fraud," less sensitive information, such as "data that can be rendered useless to cybercriminals[,] does not pose the same risk of future identity theft or fraud to plaintiffs if exposed." *McMorris*, 995 F.3d at 302; *see also, e.g.*, *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1344 (11th Cir. 2021) (Plaintiff failed to allege a substantial risk of future harm because he immediately cancelled his credit cards after the breach and any future risk was, "at best, speculative.").

D. Even if Plaintiff had any injury, he fails to plausibly link it to the Coding Error.

Even if Plaintiff had shown a sufficiently "concrete and particularized" injury, he fails to link it to the Coding Error. To establish causation for purposes of Article III, the alleged injuries must be "fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party." *Cooper v. Bonobos, Inc.*, 2022 WL 170622, at *2 (S.D.N.Y. Jan. 19, 2022) (quoting *Lujan*, 504 U.S. at 560–61). Plaintiff fails to make that showing.

As an initial matter, even taking Plaintiff's allegations at face value, there is no causal link between Plaintiff's so-called "injuries" and the Coding Error other than that the Coding Error occurred approximately six months before the first supposed "injury." The Court has already rejected as insufficient this mere "implied temporal connection." *See* MTD Decision at *7–8.

Moreover, the Court already credited Defendants' evidence that the August 2021 freeze on Plaintiff's Ally account, which purportedly caused him to "los[e] the opportunity to purchase securities at favorable market prices," AC ¶¶ 76–84, and the September 2021 "unauthorized attempt to break into Plaintiff's Ally Bank account," *id.* ¶¶ 85–86, were the result of a litigation freeze and his own use of financial aggregators, respectively; they were not the result of the Coding Error, *see* MTD Decision at *8; *see also* Decl. ¶¶ 25–31. Likewise, the new allegations that he has been locked out of his Ally account on at least two additional occasions since October 2022 (AC ¶ 113) were not the result of the Coding Error, and were instead due to a legal hold preventing the closing of one old account number which was no longer in use and so did not impact Plaintiff's ability to access his accounts or his funds. *See* Decl. ¶¶ 33–34.

Additionally—and crucially—Plaintiff's sensitive personal information has been implicated in at least *25 known data breaches* over the last several years, compromising everything from his email, passwords (which again, Plaintiff reuses), password hints, usernames, phone numbers, physical addresses, gender, date of birth, IP addresses, partial credit card data, geographic locations, social media profiles, and job titles. *See* Ex. 4. There is no legitimate reason to believe that his alleged issues with Coinbase, Amazon, and other non-Ally accounts stem from the Coding Error (which was limited only to Ally business partners) and not one of these many data breaches.

In fact, the only plausible conclusion is the opposite: that the harms of which he complains trace back to one or more of these breaches. *First*, a number of these breaches were malicious breaches orchestrated by bad actors for the express purpose of stealing personal information; indeed, some were discovered when hackers posted the stolen user information (including Plaintiff's) on popular hacking forums (*e.g.*, the TicketFly and Gemini breaches). *See* Ex. 4 at 5, 7. As the first *McMorris* factor recognizes, a data leak involving malicious hackers is far more likely to lead to identity theft and fraud than one that (like the Coding Error) does not. *See McMorris*, 995 F.3d at 303. *Second*, Plaintiff admits in his Amended Complaint that he uses the *very same password* that was supposedly leaked as a result of the Coding Error for many of his online accounts, including those with Coinbase and Amazon. *See* AC ¶¶ 109, 114. That is outrageous, causation-confounding behavior.[12] It does not follow, then, that hacking attempts utilizing his old Ally password trace back to the Coding Error; they could be the result of a breach affecting *any* of his several accounts utilizing that same password. *Third*, and relatedly, Coinbase itself reportedly suffered a data breach by malicious hackers around the same time as the Coding Error.[13] This severs any connection between the Coding Error and Plaintiff's Coinbase-related "injury." It also illustrates Plaintiff's overarching causation problem: His information, including

[12] Plaintiff cannot manufacture standing here by using the same password across numerous sites, then, knowing it may have been exposed on one website, refusing to change his password on all others for years. It is well established that a plaintiff cannot manufacture standing by "inflicting harm on themselves." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 416 (2013); *see also Taylor v. Fed. Aviation Admin.*, 2019 WL 3767512, at *4 (D.D.C. Aug. 9, 2019) ("Where a plaintiff has an 'easy means' to remedy a claimed injury, but fails to take advantage of it, such injury 'would not be fairly traceable to the defendant's challenged conduct.'"); *Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 751 (S.D.N.Y. 2017) ("Plaintiffs were not legally permitted to watch passively as their identities were stolen and bank accounts drained.").

[13] *See Silver Miller Investigating Hacked Coinbase Accounts*, Cision PR Newswire (Dec. 07, 2022), https://www.prnewswire.com/news-releases/silver-miller-investigating-hacked-coinbase-accounts-301697416.html.

his password that he apparently—and incredibly—uses across numerous online accounts, has been maliciously stolen on several occasions such that he cannot plausibly trace its misuse back to any particular one, let alone to the inadvertent, immediately rectified Coding Error.

Plaintiff lacks Article III standing and thus this Court lacks subject matter jurisdiction. The Amended Complaint must be dismissed under Rule 12(b)(1).

II. THE AMENDED COMPLAINT SHOULD BE DISMISSED UNDER RULE 12(b)(6) BECAUSE PLAINTIFF FAILS TO STATE ANY CLAIM FOR RELIEF.

Even if Plaintiff had standing (which he does not), each of his seven claims should be dismissed under Rule 12(b)(6) for failure to state a claim. To survive a Rule 12(b)(6) motion, a complaint must contain "plausible" factual allegations, taken as true, which "raise a right to relief above the speculative level." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). "The plausibility standard . . . asks for more than a sheer possibility . . . . Where a complaint pleads facts that are merely consistent with a defendant's liability, it stops short of the line between possibility and plausibility of entitlement to relief." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). The Court need not accept "legal conclusions," and "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.* at 678.

A. Choice of law.

A federal court sitting in diversity "applies the choice-of-law rules of the state in which it sits." *Andrews v. Sotheby Int'l Realty, Inc.*, 2014 WL 626968, at *4 (S.D.N.Y. Feb. 18, 2014), *aff'd*, 586 F. App'x 76 (2d Cir. 2014). New York's choice-of-law rules look to the state with the most significant interest in the litigation. *See GlobalNet Financial.com, Inc. v. Frank Crystal & Co.*, 449 F.3d 377, 384 (2d Cir. 2006). For both tort and contract claims, this analysis is "almost exclusively" based on "the parties' domiciles and the locus of the [alleged] tort." *In re Thelen LLP*, 736 F.3d 213, 219–20 (2d Cir. 2013) (tort); *AEI Life LLC v. Lincoln Benefit Life Co.*, 892

F.3d 126, 135 (2d Cir. 2018) (contract). In cases alleging unauthorized data disclosure, courts generally apply the law of the state in which the company is headquartered. *See Schmitt v. SN Serv. Corp.*, 2021 WL 3493754, at *4 (N.D. Cal. Aug. 9, 2021) (collecting cases).

The jurisdictions relevant here are Utah—where Ally Bank is headquartered—and Virginia—Plaintiff's domicile. Plaintiff's claims fail under either Utah or Virginia law.

B. Plaintiff fails to state a negligence claim (Count I).

To state a successful negligence claim, Plaintiff must allege that Defendants owed a duty to him, breach of that duty, and damages proximately caused by the breach. *See Atrium Unit Owners Ass'n v. King*, 585 S.E.2d 545, 548 (Va. 2003); *Hunsaker v. State*, 870 P.2d 893, 897 (Utah 1993). Here, among other things, Plaintiff's claim fails because he cannot demonstrate the existence of a legal duty or that he suffered any legally cognizable damages.

Plaintiff does not (and cannot) allege that Ally had a legal duty to him absent an assumption of duty by Ally. Neither Utah nor Virginia have recognized a common-law duty to protect electronic private information from unauthorized disclosure. *See Parker v. Carilion Clinic*, 819 S.E.2d 809, 826 (Va. 2018); *Deutsche Bank Nat'l Tr. Co. v. Buck*, 2019 WL 1440280, at *5 (E.D. Va. Mar. 29, 2019).[14] Instead, Plaintiff alleges that Ally assumed a duty to Plaintiff "[b]y collecting and storing [Plaintiff's] data." AC ¶ 149. But neither Utah nor Virginia have recognized any assumed duty outside the context of negligent actions causing *physical harm*. Indeed, both states have adopted Restatement (Second) of Torts § 323 as the standard for finding an assumed duty, which requires "physical harm resulting from [defendant's] failure to exercise reasonable care to perform his undertaking." *See MacGregor v. Walker*, 322 P.3d 706, 711 (Utah 2014)

[14] The Utah Supreme Court has not addressed whether Utah recognizes a common-law duty in this context and no federal or other court applying Utah law has found that Utah would do so.

("[S]ection 323, by its very terms, requires 'physical harm' from the negligently rendered services."); *Davis v. Walmart Stores E., L.P.*, 687 F. App'x 307, 311 (4th Cir. 2017) ("assumption of duty applies only in a narrow subset of Virginia cases: wrongful death, wrongful birth, and one specific type of negligent driving cases"). Here, Plaintiff does not allege any physical harm.

Even if Ally assumed a duty under either Utah or Virginia law, Plaintiff does not plausibly allege that Ally failed to use reasonable care. The mere fact that the Coding Error occurred is insufficient to infer a lack of reasonable care because negligence is not a strict liability standard. *See, e.g.*, *Bylsma v. R.C. Willey*, 416 P.3d 595, 605 (Utah 2017); *Arlington Forest Assoc. v. Exxon Corp.*, 774 F. Supp. 387, 390 (E.D. Va. 1991). Even the regulatory authorities Plaintiff cites in the Amended Complaint, such as the Federal Trade Commission, acknowledge that data exposures "sometimes can happen when a company has taken every reasonable precaution."[15] Moreover, Plaintiff does not (and cannot) allege that bad actors exploited vulnerabilities in Ally's systems or that Ally was aware of but failed to address system weaknesses. *See, e.g.*, *McCartney v. United States*, 31 F. Supp. 3d 1340, 1346 (D. Utah 2014) (dismissing negligence claim where there was no allegation that defendant "acted unreasonably in its undertaking [of duty]").

Instructive of Plaintiff's failure is *In re Capital One Consumer Data Security Breach Litigation*, 488 F. Supp. 3d 374, 400–01 (E.D. Va. 2020), in which the court found—in circumstances wholly unlike those here—that the plaintiff had stated a negligence claim under an assumed duty theory where the defendants (i) solicited potential customers' highly sensitive personal data and maintained a "data lake" of that data solely for their own business purposes unconnected with the customer; (ii) were "aware of the vulnerabilities and risks associated with

[15] *See* Fed. Trade Comm'n, *FTC Working to Protect Consumers and Businesses from Information Security Breaches* (Apr. 21, 2004), https://www.ftc.gov/news-events/press-releases/2004/04/ftc-working-protectconsumers-and-businesses-information-security.

their servers" on which the data was stored; and (iii) "acknowledged and anticipated attempts to gain unauthorized access" to the "data lake" of personal data yet "inadequately" protected against such access. *Id.* at 398–401.[16] Plaintiff does not and cannot plausibly plead anything similar here.

Regardless, Plaintiff's negligence claim still fails because he does not allege any legally cognizable damages.[17] Plaintiff's only allegations of harm are "lost time," "annoyance, inconvenience," attempts to hack his email and FanDuel accounts, freezes or restrictions on his Ally account, two instances of unauthorized (reimbursed) unrelated transactions with his Coinbase and Amazon accounts, and alleged risk of future injury from fraud or "identity theft crimes." AC ¶¶ 80–123. Although Plaintiff's failure to allege physical harm is dispositive, as discussed above, these alleged harms also fail because they are speculative. Under both Utah and Virginia law, damages must be actual and non-speculative to be cognizable and support a negligence claim. *See, e.g.*, *Seale v. Gowans*, 923 P.2d 1361, 1365 (Utah 1996) (alleged breach "causing only nominal damages, speculative harm, or the threat of future harm does not suffice to create [a] cause of action for negligence"); *Finney v. Clark Realty Capital, LLC*, 2020 WL 6948181, at *6 (E.D. Va. 2020) ("personal injury [or] property damage" required to state negligence claim under Virginia law); *see also, e.g.*, *Shafran v. Harley-Davidson, Inc.*, 2008 WL 763177, at *2 (S.D.N.Y. Mar. 20, 2008) (collecting cases from "courts across the country" recognizing that activities in "the anticipation of future injury that has not materialized" is not a "cognizable injury" for negligence and other claims). Without actual damages, Plaintiff's negligence claim fails.

[16] Though recognizing that Virginia has never recognized an assumed duty outside the context of "wrongful death, wrongful birth, or certain driving-related torts," and despite quoting Section 323's "physical harm" requirement, the Eastern District of Virginia found—inconsistent with Virginia law—an assumed duty under the facts of that case, including that defendants had intentionally and knowingly created a vulnerable "data lake" comprised of highly sensitive information. *Capital One*, 488 F. Supp. 3d at 400. There are no similar facts here.

[17] "Pleading damages to support a cause of action is distinct from pleading injury-in-fact to support standing" and subject to the higher Rule 12(b)(6) standard. *Wallace v. Health Quest Sys., Inc.*, 2021 WL 1109727, at *5 (S.D.N.Y. Mar. 23, 2021). Thus, even if "plaintiffs' allegations are sufficient to support standing, plaintiffs must also plead cognizable damages to survive [a] motion to dismiss under Rule 12(b)(6)." *Id.* at *5.

C. Plaintiff fails to state a negligence *per se* claim (Count II).

Plaintiff's negligence *per se* claim, predicated on Section 5 of the Federal Trade Commission Act ("FTCA"), fails under either Utah or Virginia law. Under Utah law, negligence *per se* applies only in cases involving "dangerous instrumentalities." *See Mitchell v. Wells Fargo Bank*, 355 F. Supp. 3d 1136, 1158 (D. Utah 2018) (dismissing claim premised on alleged violation of a privacy statute because negligence *per se* applies "only in cases involving dangerous instrumentalities"). "Dangerous instrumentalities" include, for example, "depositing and maintaining dynamite in a city . . . the operation of a steam railway . . . and of a street railway"—*i.e.*, instrumentalities "the maintenance or operation of which involved safety of life, limb, and property." *White v. Shipley*, 160 P. 441, 444 (Utah 1916). Indisputably, the FTCA—which was designed to prevent unfair or deceptive acts or trade practices (*see* 15 U.S.C. § 45(a)(1))—does not implicate any analogous "dangerous instrumentality" or involve the "safety of life, limb, and property," and thus cannot form the basis for a negligence *per se* claim under Utah law.

Similarly, under Virginia law, a negligence *per se* claim may only be premised on a statute that is expressly "enacted for public safety." *Collett v. Cordovana*, 772 S.E.2d 584, 589 (Va. 2015). "A statute enacted for public safety generally is designed to afford protection to the public against careless or reckless acts which may result in bodily injury or property damage." *Tidewater Marina Holdings, LC v. Premier Bank, Inc.*, 2015 WL 13801664, at *2 (Va. Cir. Ct. Aug. 7, 2015). The FTCA is not designed to protect against either. Indeed, confronted with this very question, a Virginia federal court, applying Virginia law, dismissed a negligence *per se* claim because the FTCA is not "expressly aimed at protecting public safety." *Capital One*, 488 F. Supp. 3d at 408. The court distinguished between public safety statutes (*e.g.*, firearm regulations) and "statutes aimed at protecting society from fraud and other dishonest conduct," which are "not the type of regulation that can support a negligence *per se* claim." *Id.* Plaintiff's claim should be dismissed.

D. Plaintiff fails to state a claim for breach of implied contract (Count III).

Plaintiff claims that he entered an "implied contract" with Ally pursuant to which Ally agreed to "undertake appropriate safeguards and data security practices and policies consistent with industry standards." AC ¶ 166. The Coding Error, Plaintiff alleges, was a breach of that implied contract. *Id.* ¶ 170. To state a claim for breach of an implied contract under either Utah or Virginia law, Plaintiff must allege all of the elements for an express breach of contract claim: (1) a legally enforceable contract (implied based on a course of conduct or "mutual assent"); (2) breach; and (3) damages. *See Eleopulos v. McFarland & Hullinger LLC*, 145 P.3d 1157, 1159 (Utah Ct. App. 2006); *Filak v. George*, 594 S.E.2d 610, 619 (Va. 2004). Plaintiff's claim fails.

Plaintiff's attempt to derive an implied contract from the Ally website "policies" and slogans (*e.g.*, "keeping accounts and personal information secure is a top priority for us") (*see* AC ¶¶ 55–74) falls far short of alleging an enforceable agreement. Such general statements about Ally's intentions lack specificity in terms and conditions required for an enforceable agreement. *Heideman v. Wash. City*, 155 P.3d 900, 908 (Utah Ct. App. 2007) (implied contract requires "an intention to make a bargain with certain terms or terms which reasonably may be made certain"); *Willner v. Dimon*, 2015 WL 12766135, at *4 (E.D. Va. May 11, 2015) (website statements must be "clear, definite, and explicit, and leave[] nothing open for negotiation" to be enforceable).

Further, Plaintiff does not adequately allege any non-speculative damages attributable to the purported failure to "undertake appropriate safeguards." AC ¶ 166. "Damages based on uncertainties, contingencies, or speculation cannot be recovered," and "[t]he failure to establish damages with reasonable certainty warrants the dismissal of a breach of contract claim." *Isle of Wight County v. Nogiec*, 704 S.E.2d 83, 85–86 (Va. 2011); *R4 Constructors LLC v. Inbalance Yoga Corp.*, 480 P.3d 1075, 1082 (Utah Ct. App. 2020) ("The court determined that the lack of causation evidence made [defendant]'s claim for damages speculative and that [defendant] therefore could not prove damages as a matter of law."). Here, the closest Plaintiff comes to alleging some actual, unreimbursed economic harm is that he missed out on the opportunity for advantageous investment opportunities. AC ¶ 82. But he fails to plausibly connect the August 2021 lockout that purported led to this inability to capitalize on investment opportunities to the purported failure to undertake appropriate safeguards. Moreover, even if he had adequately alleged a causal connection, a missed opportunity to invest at advantageous prices is not a reasonably foreseeable consequence of the failure to "undertake appropriate safeguards and data security practices and policies." *Id.* ¶ 166. This, too, is fatal to his claim. *See Long v. Abbruzzetti*, 487 S.E.2d 217, 219 (Va. 1997) ("[I]f damages are consequential in nature, they are compensable only if the special circumstances were within the contemplation of all contracting parties at the time the contract was made . . . 'Contemplation,' in this context, includes both circumstances that are actually foreseen and those that are reasonably foreseeable."); *Trans-Western Petroleum, Inc. v. U.S. Gypsum Co.*, 379 P.3d 1200, 1202 (Utah 2016) (similar).

Finally, because there was indisputably a comprehensive, *express* contract governing the relationship between Plaintiff and Defendants (*see* Decl. Ex. A), Plaintiff cannot now assert a cause of action for breach of an *implied* contract to circumvent those express rights and obligations or lack thereof. *See Gunderson v. Petersburg Hosp. Co., LLC*, 2016 WL 11575139, at *3 (Va. Cir. Ct. Jul. 13, 2016) ("There is no dispute that an express contract existed between the parties. The existence of an enforceable contract precludes Gunderson from proceeding on a theory of implied contract. [Plaintiff]'s claim for breach of implied contract is inadequate as a matter of law."); *U.P.C., Inc. v. R.O.A. Gen., Inc.*, 990 P.2d 945, 955 (Utah Ct. App. 1999) ("An express agreement or covenant excludes the possibility of an implied one of a different or contradictory nature.").

E. Plaintiff fails to state a claim for breach of fiduciary duty (Count IV).

Plaintiff fails to plead any of the elements necessary for his fiduciary duty claim: a fiduciary relationship, a breach, causation, and damages. *See Carstensen v. Chrisland Corp.*, 442 S.E.2d 660, 666 (Va. 1994); *Gables at Sterling Vill. Homeowners Ass'n v. Castlewood-Sterling Vill. I, LLC*, 417 P.3d 95, 109 (Utah 2018). First, Plaintiff *expressly agreed* there was no fiduciary relationship between him and Ally (*see* Decl. Ex. A at 9 ¶ 2), which is fatal. *See Sun Hotel v. Summitbridge Credit Invs. III, LLC*, 2013 WL 8019584, at *5 (Va. Cir. Ct. 2013). Even setting aside that express agreement, Defendants were not fiduciaries for Plaintiff because there was no "special confidence" between them akin to that of attorney-client or insurer-insured. *See Lattimore v. Brahmbatt*, 2022 WL 16914528, at *5 (W.D. Va. Nov. 14, 2022) ("[A]n ordinary relationship between a bank and its customer does not give rise to a fiduciary duty."); *First Sec. Bank N.A. v. Banberry Dev. Corp.*, 786 P.2d 1326, 1333 (Utah Sup. Ct. 1990) (being a customer of a bank "is insufficient, by itself, to establish a fiduciary relationship"). Even if there was a fiduciary relationship, there was no breach, no causation, and no damages. *See supra* Sections I, II.B.

F. Plaintiff fails to state a claim for violation of NCUDTPA (Count V).

Plaintiff's bare-bones claim under the North Carolina Unfair & Deceptive Trade Practices Act ("NCUDTPA"), pursuant to which he claims Ally made "deceptive" and "misleading" statements about its data security (AC ¶¶ 179–84) fails because the NCUDTPA applies only to conduct with a sufficient nexus to North Carolina, and Plaintiff fails to adequately link the alleged wrongdoing under the NCUDTPA to North Carolina. *The 'In' Porters, S.A. v. Hanes Printables, Inc.*, 663 F. Supp. 494, 501 (M.D.N.C. 1987) (NCUDTPA "requires an in-state injury to plaintiff before plaintiff can state a valid unfair trade claim"). Plaintiff does not allege that the supposedly "deceptive" and "misleading" statements were made to him in North Carolina. Rather, he vaguely alleges only that certain employees with no clear connection to this dispute and some "website and computer systems" were "based" in the state. AC ¶¶ 31–33. This disconnect alone requires dismissal. *See Verona v. U.S. Bancorp*, 2011 WL 1252935, at *15 (E.D.N.C. Mar. 29, 2011) (dismissing claims against non-N.C. entities on extraterritoriality basis).

Plaintiff's NCUDTPA claim also fails because he does not adequately allege that Ally's actions were "immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers." *Manos v. Freedom Mortg. Corp.*, 2022 WL 874181, at *2 (4th Cir. Mar. 24, 2022). Nor could he: If, as Plaintiff suggests, it was the fact of the Coding Error that makes Ally's data-security statements "deceptive" and "misleading," and yet those statements were made *before* the Coding Error, then those statement *could not have been* "deceptive" or "misleading." And Plaintiff concedes that the Coding Error was a mere "malfunction[]" (AC ¶ 48)—a mistake—not the sort of deceptive act necessary to state a NCUDTPA claim. *See Edwards v. Genex Coop., Inc.*, 777 F. App'x 613, 622 (4th Cir. 2019) ("mere mistake" is generally insufficient under NCUDTPA).

Additionally, Plaintiff wholly fails to allege actual damages attributable to these purported "deceptive" and "misleading" statements, also requiring dismissal. *See Belcher v. Fleetwood Enters.*, 590 S.E.2d 15, 18 (N.C. Ct. App. 2004) (to recover under the NCUDTPA, "plaintiffs must prove they suffered actual injury as a result of defendants' unfair and deceptive act").

G. Plaintiff fails to allege a violation of VPIBNA (Count VI).

Plaintiff claims Ally violated the Virginia Personal Information Breach Notification Act ("VPIBNA") because it did not "disclose" the Coding Error in a "timely" manner. AC ¶ 191. VPIBNA provides that entities that possess the "personal information" of a Virginia resident must provide notification "without unreasonable delay" of any "breach of the security of its system." Va. Code § 18.2-186.6(B). Plaintiff's claim fails under the statute's plain language.

First, the information Plaintiff alleges was disclosed as a result of the Coding Error is not "personal information" under the VPIBNA. The VPIBNA defines "personal information" as "the first name or first initial and last name in combination with and linked to any one or more of" certain "data elements" (*e.g.*, SSN, passport number, financial account number) when "the data elements are neither encrypted nor redacted." Va. Code § 18.2-186.6(A).[18] Under the plain terms of the statute, Plaintiff's self-selected username and password are not "personal information."

Second, Plaintiff's claim also fails because he has not alleged a "breach of the security of the system"[19] as Plaintiff has not alleged that the Coding Error "has caused" or "reasonably . . . will cause" him to suffer identity theft or fraud. *See supra* Section I.

Third, Plaintiff's claim fails because, even if there had been a "breach of the security of the system" with respect to "personal information" (there was not), Plaintiff cannot plausibly allege that Defendants "unreasonably delay[ed]" in providing notice of the Coding Error. *Id.* § 18.2-186.6(A), (B). The VPIBNA does not define "unreasonable delay," but it is a fact-specific inquiry. *See Capital One*, 488 F. Supp. 3d at 389 (four months was unreasonable); *Griffey v. Magellan Health Inc.*, 562 F. Supp. 3d 34, 57 (D. Ariz. 2021) (one month was reasonable). The time between discovery of the Coding Error on April 12, 2021 and the June 11, 2021 notification letter was necessary—and thus reasonable—since Ally had to parse millions of login attempts to identify any affected customers. Regardless, Ally immediately forced a password reset. Plaintiff cannot plausibly allege that it was unreasonable for Ally to notify only actually affected customers.

Finally, Plaintiff's claim fails because Plaintiff has not alleged "direct economic damages." *See* Va. Code § 18.2-186.6(I). Indeed, as discussed *supra* Section I, Plaintiff has failed to allege *any* damages, let alone *economic* damages. *See Corona v. Sony Pictures Enter., Inc.*, 2015 WL 3916744, at *8 (C.D. Cal. 2015) (VPIBNA claim fails without "economic damages").

[18] The statutory data elements are: "1. Social security number; 2. Driver's license number or state identification card number issued in lieu of a driver's license number; 3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts; 4. Passport number; or 5. Military identification number." Va. Code § 18.2-186.6(A).

[19] The definition is: "[T]he unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud." *Id.*

H. Plaintiff fails to state a claim for injunctive/declaratory relief (Count VII).

Plaintiff claims he is entitled to injunctive or declaratory relief under the Declaratory Judgment Act (the "DJA"), 28 U.S.C. § 2201, based on speculation that "there is no reason to believe that the Defendants' security practices are any more adequate now" than when the Coding Error occurred. AC ¶ 205. To obtain declaratory or injunctive relief, Plaintiff must plausibly allege entitlement to relief on an underlying claim. *See, e.g.*, *Chevron Corp. v. Naranjo*, 667 F.3d 232, 244 (2d Cir. 2012) (declaratory relief requires a "valid legal predicate"). Because the Amended Complaint fails to state any claim for relief, Plaintiff is precluded from seeking declaratory or injunctive relief. *See Chiste v. Hotels.com L.P.*, 756 F. Supp. 2d 382, 406 (S.D.N.Y. 2010) ("Declaratory judgments and injunctions are remedies, not causes of action.").[20]

Regardless, Plaintiff's claim still fails for the same reasons that undergird its lack of standing. "[T]o establish standing to obtain prospective relief, a plaintiff must show a likelihood that he will be injured in the future." *Carver v. City of New York*, 621 F.3d 221, 228 (2d Cir. 2010). Plaintiff cannot do so here for the same reasons described *supra* Section I. Moreover, Plaintiff does not allege any injury as to which there is any "likelihood" of being "harmed again in the future in a similar way," nor that he faces any likelihood of future injury due to the Coding Error. *Nicosia v. Amazon.com, Inc.*, 834 F.3d 220, 239 (2d Cir. 2016); *see supra* Section I.

CONCLUSION

The Amended Complaint should be dismissed in its entirety with prejudice.[21]

[20] Moreover, certain of Plaintiff's claims cannot support injunctive relief as a matter of law. *See Patton v. Experian Data Corp.*, 2018 WL 6190349, at *11 (C.D. Cal. Jan. 23, 2018) ("The injunction remedy does not appear in section 18.2-186.6 [VPIBNA]. Thus, there can be no private right of action for injunctive relief.").

[21] Plaintiff has had multiple chances to cure his pleading deficiencies. He has not and cannot do so, and his Amended Complaint should be dismissed with prejudice. *See Phadnis v. Tata Am. Int'l Corp.*, 2021 WL 3374542, at *2 (S.D.N.Y. Aug. 3, 2021) (denying leave to amend and dismissing case with prejudice because "Plaintiff has had two opportunities to amend his complaint and has failed to cure the numerous previously-identified deficiencies").

Dated: March 6, 2023
New York, New York

SIMPSON THACHER & BARTLETT LLP

By: /s/ *Martin S. Bell*
Martin S. Bell
Rachel S. Sparks Bradley
Patrick K. Barry
425 Lexington Avenue
New York, New York 10017
Telephone: (212) 455-2000
Facsimile: (212) 455-2502
martin.bell@stblaw.com
rachel.sparksbradley@stblaw.com
patrick.barry@stblaw.com

Attorneys for Defendants Ally Bank and Ally Financial Inc.